We claim:

1. A wired network for providing secure, authenticated access to wireless network clients, comprising:

a server connected to a wireless network access point, the server being operative to perform authentication for wireless clients establishing a connection to the server through the wireless network access point, the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client, the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key valid for the connection session to the client upon authentication of the client; and

a user database accessible to the server for use in validating wireless clients.

2. The wired network according to claim 1 and also including a network hub providing connections between the server and additional resources on the wired network.

3. The wired network according to claim 1 and also including a router providing connections between the server and additional resources on the wired network as well as a connection to an additional wired network.

4. The wired network according to claim 2 wherein the server is operative to provide addresses to clients through dynamic host control protocol.

5. The wired network according to claim 4 wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol.

6. The wired network according to claim 5 wherein the server employs 128-bit cryptoprocessing to communicate with the wireless network client.

7. A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising:

a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network, the wireless network access point being operative to conduct communications with the server, the wireless network access point being further operative to receive authentication information from clients and transfer the authentication information to the server and to receive a cryptoprocessing key from the server and transfer the key to each of the clients; and

a plurality of wireless network clients operative to establish connections with the wireless network access point, each client being operative to conduct encrypted communications with the server through the access point, to pass authentication information to the network access point and receive address information and cryptoprocessing data from the network access point to allow communication with the wired network, each client being operative to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and cryptoprocessing information.

8. The wireless network of claim 7 wherein the access point communicates with the server using point to point tunneling protocol.

9. The wireless network of claim 8, also including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and the additional network access points being operative to establish connections with the server through the network hub.

10. A method of secure communication between wireless network clients and a wired network, comprising the steps of:

establishing a connection between an SB server connected to the wired network and a wireless network access point;

establishing a connection between the SB server and a network client communicating with the SB server through the wireless network access point;

exchanging encryption keys between the SB server and the wireless network client;

performing authentication for the wireless network client;

if authentication fails, rejecting connection to the wired network; and

if authentication passes, accepting connection to the wired network, providing a temporary wired network address and a unique session encryption key to the wireless network client and providing access to wired network resources in response to requests by the wireless network client.

11. The method of claim 10 wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection and wherein the step of accepting the connection is accompanied by a step of logging the acceptance.

12. The method of claim 11 wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address.

13. The method of claim 12 wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol.

14. The method of claim 13 wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless

network client and the SB server and wherein the authentication information is encrypted using public key cryptography.

15. The method of claim 14 wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key using public key cryptography.